COUNTY OF LOS ANGELES
CHIEF INFORMATION OFFICE
500 West Temple Street
493 Kenneth Hahn Hall of Administration
Los Angeles, CA 90012

JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

Telephone: (213) 974-2008
Facsimile: (213) 633-4733

August 16, 2006

To: Mayor Michael D. Antonovich
Supervisor Zev Yaroslavsky, Chair Pro Tem
Supervisor Gloria Molina
Supervisor Yvonne B. Burke
Supervisor Don Knabe

From: Jon W. Fullinwider
Chief Information Officer

Subject: **COMPUTER SECURITY INCIDIENTS AT COMMUNITY DEVELOPMENT COMMISSION (CDC) AND DEPARTMENT OF COMMUNITY AND SENIOR SERVICES (DCSS)**

On July 21, 2006, I advised your Board that an Internet-based attack had accessed a Community Development Commission (CDC) computer system and potentially exposed approximately 4,800 Housing Management Division tenants' personal information to access by unknown persons or organizations. CDC retained the services of a forensic expert to determine what was accessed and what vulnerabilities existed enabling the event to occur. The investigation has been completed and concludes with a high degree of certainty that no CDC tenant records were accessed or exposed. Therefore, CDC will not be required to send notices to individuals whose personal information was contained in the subject system.

On the weekend of July 22-23, the Department of Community and Senior Services' (DCSS) Burbank and Glendale offices were burglarized, along with other tenants in the building. In this particular event, 11 DCSS laptop computers were stolen. As stated in my previous report, these laptops contained personal information on 216 DCSS constituents. Letters have been sent to these individuals notifying and instructing them regarding precautions they should take. Credit fraud notices have also been placed in their files at major credit agencies.

My Office, in conjunction with department security officers, is developing processes that can be employed within the County to mitigate the impact of these types of events.

Three policies are in the review process prior to your Board's approval:

- Protection of Information on Portable Computing Devices
- Security Incident Reporting
- Employee Security Awareness

Each of these policies is required to improve protection of County sensitive information. The policy for information on portable computing devices will require that all information (sensitive/confidential as well as all other types of information) be encrypted when downloaded to portable computing devices. This implies that all laptop computers must have full disk encryption regardless of the type of information contained on them. We have also commissioned a County technical team to complete requirements for a County encryption standard and have developed a Request for Proposal (RFP) to secure the required software. The policies are being coordinated with the various involved County agencies prior to submittal to your Board. The encryption software acquisition is proceeding through the RFP process with vendor responses due within the first two weeks of September.

My Office will continue to monitor progress by the involved departments to ensure that risk mitigation efforts are completed. Additionally, we have made it our top priority to complete the policies and implement the encryption software on portable computers for the entire County.

This memorandum will close the existing incident and no further reports will be developed.

JWF:ygd

Attachments

c: Cynthia D. Banks, Director, DCSS
Al Brusewitz, CISO, Chief Information Office
Raymond Fortner, County Counsel
Sachi A. Hamai, Executive Officer, Board of Supervisors
Carlos Jackson, Executive Director, CDC
David E. Janssen, Chief Administrative Officer
J. Tyler McCauley, Auditor-Controller